Sécurité des communications 5G véhiculaires (5G-V2X) dans un contexte transfrontalier

Abdelwahab Boualouache, Sidi-Mohammed Senouci, Bouziane Brik, Shajjad Hossain, Qiang Tang, Abdelaziz Amara Korba, Rami Langar, Sylvain Cherrier, Badre Bousalem, Vinicius F Silva, et al.

Sécurité des communications 5G véhiculaires (5G-V2X) dans un contexte transfrontalier

Abdelwahab Boualouache[1], Sidi-Mohammed Senouci[2], Bouziane Brik[2], Shajjad Hossain[2], Qiang Tang[3], Abdelaziz Amara Korba[4], Rami Langar[5], Sylvain Cherrier[5], Badre Bousalem[5], Vinicius F. Silva[5], Yacine Ghamri-Doudane[4], et Thomas Engel[1]

[1] FSTM, Université du Luxembourg, Luxembourg
[2] Laboratoire DRIVE EA1859, Université de Bourgogne France
[3] Luxembourg Institute of Science and Technology (LIST), Luxembourg
[4] La Rochelle Université, Laboratoire L3I, France
[5] Laboratoire LIGM - UMR 8049, Université Gustave Eiffel, France

Peut-on faire confiance aux véhicules du futur munis d'une connexion 5G ? Si la connectivité accrue grâce à la technologie du « *slicing* » ouvre de réelles opportunités, un certain nombre de failles de sécurité potentielles sont également à considérer, notamment lors d'un basculement d'opérateur dans une zone frontalière. A partir de l'étude de 3 cas concrets d'usage cet article analyse les risques et les solutions possibles.

Introduction

La 5G embarquée va transformer l'expérience des usagers dans le secteur du transport, et plus particulièrement dans nos voitures, afin de rendre nos voyages plus efficients et plus sûrs. En effet, l'industrie automobile devrait subir deux évolutions majeures qui nécessiteront un réseau plus robuste, plus stable et à faible latence : le développement tout d'abord des services de gestion du trafic et de sécurité routière, puis à terme celui de la conduite automatisée [1]. Ce réseau permettra l'échange aussi bien entre les véhicules (V2V[1]), entre les véhicules et une infrastructure routière

1 *Vehicle-to-Vehicle*

(V2I [2]), ou encore entre les véhicules et des serveurs distants (V2N [3]), voire les piétons ou plus largement tous les usagers vulnérables de la route (V2P [4]). Ceci est possible grâce à la technologie radio de la 5G qui offre deux interfaces de communication : l'interface Uu utilisée pour les communications V2N et l'interface *PC5* [5] pour les communications directes V2V, V2P et V2I [2]. Ainsi les voitures pourront «voir» plus loin sur la route et ainsi mieux percevoir leur environnement proche et lointain, anticiper les risques et fluidifier le trafic.

Les opportunités offertes par la 5G-V2X devraient donner naissance dans un futur proche à de nouveaux services, qui tireront profit des possibilités offertes par la 5G, comme une latence ultra-faible, une grande fiabilité de communication, une large bande passante, la prise en charge d'un nombre important de véhicules autonomes et connectés (VAC), et une connectivité fiable dans des conditions de forte mobilité [1]. Ce déploiement ne sera possible qu'avec l'adoption généralisée de la technologie 5G, dans sa version autonome (SA), grâce, notamment, au découpage en tranches de réseau [6], au Réseau Défini par Logiciel [7] (SDN) et à la Virtualisation des Fonctions Réseau (NFV [8]) [3].

A l'instar de la virtualisation apparue dans le monde des services de stockage et de calcul et qui a donné naissance au *cloud*, le *slicing* permet de construire plusieurs réseaux logiques indépendants et virtualisés à partir d'une même infrastructure de réseau physique. Pour ce faire, le *slicing* tire parti des technologies SDN et NFV. Chaque tranche de réseau est ainsi un réseau isolé de bout en bout conçu pour répondre aux différentes exigences d'une application véhiculaire particulière. Par conséquent, le concept de *slicing* permet la coexistence d'un large éventail d'applications véhiculaires partageant une infrastructure de réseau commune. Cependant, sa mise en œuvre dans le réseau véhiculaire entraîne de nouveaux défis et exigences en matière de cybersécurité, qui n'ont pas encore été prises en compte, que ce soit par les normes automobiles [4] ou par les normes 5G [5]. Sans mesures spécifiques de cyber protection, le *slicing* ouvrirait ainsi la voie à de nouvelles attaques potentielles qui viendraient s'ajouter à la pléiade d'attaques déjà connue et plus ou moins maîtrisée qui visent les véhicules connectés. Les nouveaux attaquants pourraient exploiter le maillon le plus faible de la chaîne, les véhicules autonomes et connectés, pour violer l'isolation que procure le *slicing* et dégrader les performances d'une tranche entière du réseau. Ainsi, attaquer un seul véhicule pourrait engendrer des situations dangereuses pour l'ensemble des passagers et conducteurs impliqués dans cette tranche. De surcroit, le contexte de dérégulation européenne des télécoms, fait que les attaques sur le *slicing* véhiculaire peuvent être plus importantes dans les zones transfrontalières où les véhicules transitent d'un pays à l'autre et donc d'un réseau à un autre [6].

" A l'instar de la virtualisation apparue dans le monde des services de stockage et de calcul et qui a donné naissance au cloud, le slicing permet de construire plusieurs réseaux logiques indépendants et virtualisés à partir d'une même infrastructure de réseau physique. Pour ce faire, le slicing tire parti des technologies SDN et NFV. "

Dans ce contexte, cet article fournit tout d'abord une vue d'ensemble des services 5G-V2X émergents utilisant du slicing et les défis potentiels de cybersécurité qui leurs sont associés, en se concentrant davantage sur les zones transfrontalières. Nous nous concentrerons sur trois services : l'insertion/dépassement automatique de voies, la régulation du flux de trafic en temps réel et la protection des usagers vulnérables de la route tels que les piétons et les cyclistes (nous les appelons par la suite VRU [9]). Ce travail apporte une analyse approfondie des questions de cybersécurité à différents niveaux, en y intégrant des questionnements relatifs à l'infrastructure 5G et aux services véhiculaires tout en se positionnant dans un contexte transfrontalier. Nous abordons également les principaux défis techniques, les questions ouvertes et les futures orientations que la recherche doit apporter face à ces vulnérabilités.

Cas d'usage émergents 5G-V2X

À ce jour, de nombreux cas d'usage 5G-V2X ont été imaginés pour un déploiement à plus ou moins court terme [7]. Afin d'illustrer nos discussions et analyses, nous avons choisi les trois cas d'usage exploitant le *slicing* dans un contexte transfrontalier illustrés par la figure 1. Il convient de mentionner que ces cas d'usage sont au cœur de notre projet de recherche 5G-INSIGHT [10]. La partie supérieure de cette figure montre le réseau cœur 5G et la couche de trai- ●●●

2 *Vehicle-to-Infrastructure*

3 *Vehicle-to-Network*

4 *Vehicle-to-Pedestrian*

5 Aussi connue sous le nom de *Sidelink*

6 *Network Slicing* – NS ou simplement *slicing*

7 *Software-Defined Networking*

8 *Network Functions Virtualization*

9 *Vulnerable Road Users*

10 http://5g-insight.eu/

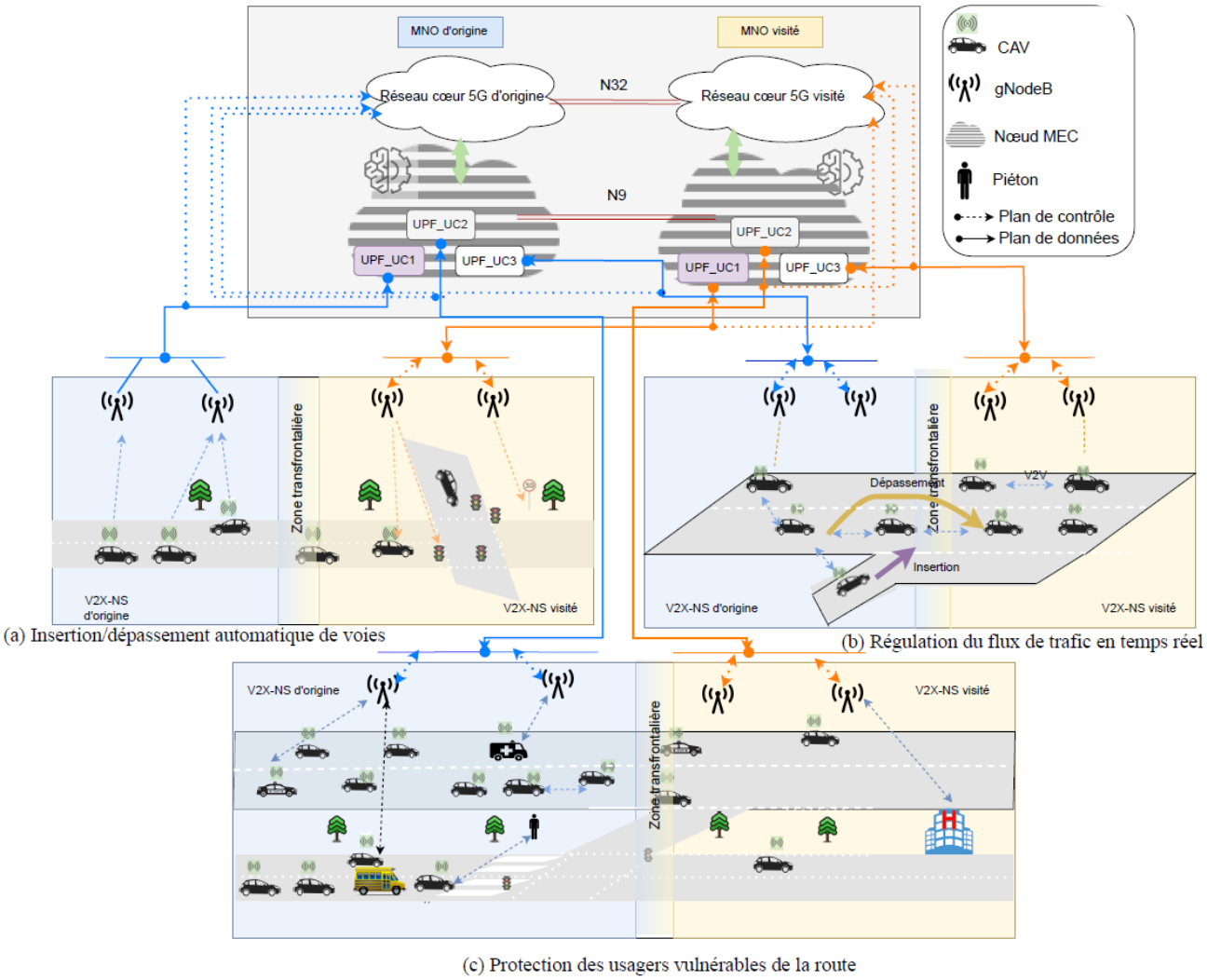

Figure 1 : Cas d'usage 5G-V2X dans une zone transfrontalière.

tement MEC [11] des opérateurs de réseaux mobiles (domestique et visité). Le scénario transfrontalier diffère du scénario général multi-opérateurs car l'opérateur d'origine et l'opérateur visité sont soumis à des politiques et des réglementations différentes, qui peuvent avoir un impact direct sur la sécurité. Par exemple, les politiques et réglementations concernant certains outils et technologies, comme la *Blockchain* ou les procédures de traitement des données, peuvent limiter les opérateurs mobiles dans la conception de solutions de sécurité efficaces. Par conséquent, dans le scénario transfrontalier, les opérateurs mobiles doivent harmoniser leurs solutions de sécurité de différents niveaux afin de respecter les politiques et réglementations des pays d'accueil. En plus, comme le montre la figure, l'isolation entre les services de *slicing* véhiculaire se fait uniquement dans le plan de données, c'est-à-dire que chaque service a une fonction UPF [12] dédiée hébergée dans la couche MEC. Lorsqu'un véhicule traverse la frontière, l'opérateur visité attribue une tranche V2X avec la même fonctionnalité que dans la tranche de l'opérateur d'origine. N9 et N32 sont des points de référence donnés par les normes 5G respectivement entre deux UPF, et entre le réseau cœur 5G visité et le réseau d'origine. Dans chaque service, le *gNodeB* [13] est rattaché à l'UPF attribué pour le plan de données et au réseau cœur 5G pour le plan de contrôle. Dans ce qui suit, nous décrivons le fonctionnement précis de ces trois cas d'usage.

Premier cas d'usage : Insertion/dépassement automatique de voies

Ce cas d'usage, illustré sur la figure 1 (a), est adapté au contexte autoroutier. Il permet aux véhicules autonomes et connectés (VAC) de déterminer les meilleures manœuvres d'insertion/dé-

11 *Mobile Edge Computing*

12 *User Plane Function*

13 Nom de la station de base en 5G

passement, c'est à dire les plus sûres, en fonction de la situation. Les VACs perçoivent leur environnement en recueillant des informations sur la position sur la voie, l'accélération, la vitesse, la taille, etc. Ils peuvent collecter ces données à la fois par le biais de leurs équipements embarqués (capteurs, caméras, radars, lidars, etc.), ainsi que par des capteurs installés au bord des routes ou par ceux des véhicules voisins. Ensuite, ces données sont traitées localement ou au niveau d'un nœud périphérique MEC pour prendre les décisions appropriées concernant les manœuvres d'insertion/dépassement de voies. La tranche dédiée à ce service doit assurer une communication fiable et à faible latence entre les véhicules et l'infrastructure 5G, en particulier dans les zones transfrontalières, où des procédures de routine, telles que le *handover* et l'itinérance, se produisent pour basculer d'un opérateur (l'opérateur d'origine) à un autre (l'opérateur destination). Les attaques pourraient être fatales, en particulier lorsque les véhicules circulent à grande vitesse puisque plus la vitesse est élevée, plus le choc est violent en cas d'accident et plus les conséquences sont graves.

Second cas d'usage : Régulation du flux de trafic en temps réel

Dans ce cas d'usage, nous visons à réguler le trafic dans un environnement urbain ou péri-urbain, comme le montre la figure 1 (b). Les nœuds périphériques MECs collectent en permanence des données sur le trafic routier actuel à partir des véhicules autonomes et connectés et des capteurs de bord de route. Ils traitent ensuite les données pertinentes à l'aide d'algorithmes avancés d'apprentissage automatique et de techniques d'exploration de données. Après cela, les nœuds MEC prennent des décisions pour réguler le flux de trafic comme la synchronisation des feux de circulation et l'adaptation des panneaux de signalisation variables en conséquence. Ces nœuds peuvent également envoyer des notifications aux véhicules sur les conditions de circulation et des recommandations pour améliorer la circulation. La tranche dédiée à ce cas d'usage doit être capable de gérer les données massives reçues et de les stocker dans les nœuds MEC. Ces derniers jouent un rôle essentiel, ce qui en fait des cibles idéales pour les attaquants qui veulent perturber le système de *slicing* véhiculaire. Les attaques contre les nœuds MEC peuvent entraîner des perturbations du trafic routier, des embouteillages, voire même des accidents aux carrefours. Les conséquences peuvent être importantes pour les travailleurs qui, quotidiennement, traversent des frontières situées en zone urbanisées, avec des zones de chevauchement entre plusieurs opérateurs. La quantité importante de données récoltée, stockée et traitée au niveau MEC permet aussi aux attaquants d'accéder à des informations sensibles, ce qui entraîne de graves problèmes de confidentialité.

" Lorsqu'un véhicule traverse la frontière, l'opérateur visité attribue une tranche V2X avec la même fonctionnalité que dans la tranche de l'opérateur d'origine. N9 et N32 sont des points de référence donnés par les normes 5G respectivement entre deux UPF, et entre le réseau cœur 5G visité et le réseau d'origine. "

Troisième cas d'usage : Protection des VRUs

Comme le montre la figure 1 (c), ce service concerne directement les piétons et les cyclistes. Il faut également y ajouter les véhicules spéciaux, tels que la police, les ambulances et les bus scolaires. Les données sur les usagers/véhicules spéciaux sont continuellement recueillies et stockées dans des nœuds MEC à la périphérie du réseau. Ils offrent des outils analytiques avancés pour traiter l'information recueillie. Ces informations traitées peuvent servir, par exemple, à :

- classer par ordre de priorité et faciliter le passage des VRUs ;

- classer par ordre de priorité les informations envoyées par les véhicules spéciaux, comme celles envoyées par les ambulances à l'hôpital ou les véhicules de police au poste de police ;

- permettre aux véhicules spéciaux, telles que les voitures de police et les ambulances traversant la frontière, de recevoir et de répondre aux données provenant du nœud MEC hôte. Cela pourrait permettre de gagner du temps et de sauver des vies ;

- adapter la trajectoire des véhicules qui traversent la frontière, afin d'éviter les zones avec plus de VRUs, ce qui réduirait la durée du trajet et éviterait des accidents.

Le *slicing* 5G-V2X prendrait alors en charge ce service via une réservation de ressources réseau et de stockage spécifique à ces usagers/véhicules spéciaux. Les nœuds MEC jouent également un rôle essentiel dans ce cas d'usage. Ainsi, le *slicing* 5G-V2X dans ce contexte fait apparaître les mêmes vulnérabilités et problèmes de cybersécurité et de confidentialité que ceux décrits dans le second cas d'usage. Néanmoins, les informations traitées ici sont encore plus sensibles. Elles sont traitées en dehors du réseau routier. Les attaquants seront alors tentés d'engendrer une violation voire une rupture complète du système pour obtenir le maximum de dommages. ●●●

Sécurité et vie privée dans des zones transfrontalières

Nous abordons dans cette section, tout d'abord, les préoccupations générales en matière de sécurité pouvant affecter les services véhiculaires utilisant la 5G, puis nous évoquons des attaques possibles contre le *slicing* véhiculaire, et enfin nous soulignons quelques défis de sécurité spécifiques au *slicing* véhiculaire dans des zones transfrontalières.

Préoccupations liées à la 5G

Malgré les mécanismes de sécurité actuels, des chercheurs ont montré que diverses menaces existent [9] en mettant en évidence des problèmes tels que les vulnérabilités des composants logiciels intégrés. En ce qui concerne le *slicing*, les auteurs de [10] présentent plusieurs problèmes de sécurité dans la 5G couvrant le cycle de vie, les aspects *intra-slice* et *inter-slice*. La société *Adaptive Mobile Security* a publié un rapport [14] qui souligne que de nouvelles approches sont nécessaires pour atténuer les vulnérabilités, notamment l'extraction des données des utilisateurs, les attaques par déni de service DoS [15] et l'accès illégitime aux données dans les tranches de réseau. Le rapport de l'ENISA [16] examine les menaces de sécurité contre les technologies SDN et souligne qu'une menace d'exploitation d'API peut entraîner une divulgation non autorisée, une compromission de l'intégrité ou une destruction des informations, ou une destruction/dégradation non autorisée du service.

Il convient de souligner que la 5G introduit de nouveaux mécanismes et procédures de sécurité, tout en gardant certains mécanismes et procédures antérieurs. En particulier, les opérateurs mobiles ont la possibilité de déterminer le mécanisme à utiliser en fonction de leur politique propre. Il ne sera pas surprenant que certains opérateurs continuent à utiliser les anciens mécanismes de sécurité, même s'ils sont moins sûrs ou moins robustes que les nouveaux. Au niveau de l'Union Européenne, l'ENISA a mis au point une boîte à outils 5G [17] qui contient des mesures stratégiques et techniques. Ces mesures aident les régulateurs nationaux et les opérateurs mobiles (et leurs partenaires tels que les fournisseurs de *cloud* et de services) à atteindre un objectif de sécurité paneuropéen. En outre, la boîte à outils décrit également un ensemble d'actions de soutien pour favoriser la réalisation des objectifs de sécurité. Malgré les efforts déployés, l'application de cette boîte à outils varie considérablement au sein de l'UE [18] , faisant apparaître des problèmes de sécurité potentiels dans les scénarios transfrontaliers, comme ceux décrits dans cet article.

> **" Malgré les mécanismes de sécurité actuels, des chercheurs ont montré que diverses menaces existent en mettant en évidence des problèmes tels que les vulnérabilités des composants logiciels intégrés."**

Exemples d'attaques contre le *slicing* véhiculaire

En ce qui concerne les réseaux V2X, il existe une pléthore de types d'attaque qui ciblent différents composants ou mécanismes internes. Dans notre analyse, nous avons sélectionné des attaques liées au *slicing* véhiculaire qui sont critiques pour les cas d'usages évoqués.

• **Déni de service de tranches - DoSS** [19] **:** le DoSS est une classe particulière d'attaques de déni de services (DoS) ciblant les tranches du réseau V2X et visant à épuiser directement ou indirectement leurs ressources. Par exemple, un attaquant peut injecter de multiples messages en utilisant de fausses identités, attaque connue sous la dénomination attaque *Sybil*, ce qui dégradera les performances de la tranche réseau sous-jacente et celles des autres tranches réseau qui partagent la même infrastructure physique. Dans les scénarios DoSS distribués, plusieurs nœuds malveillants au sein d'une ou de plusieurs tranches de réseau peuvent collaborer et se synchroniser pour mener l'attaque. Cette attaque peut être plus difficile à détecter si les attaquants appartiennent à plusieurs tranches de réseau V2X.

• **Attaque par usurpation d'identité du gestionnaire de tranches de réseau** [20] **:** le gestionnaire de tranches est le composant central du *slicing* réseau, qui est chargé de la gestion du cycle de vie des tranches réseau. Le placement du gestionnaire de tranches à proximité des véhicules (par exemple, au niveau MEC) offre un meilleur temps de réponse. Cependant, cela augmente le risque d'attaques par usurpation d'identité. Par exemple, un attaquant peut se faire passer pour un gestionnaire de tranches afin de monopoliser les ressources de la tranche à son profit.

• **Accès non autorisé aux tranches :** cette attaque utilise deux ou plusieurs véhicules malveillants attachés à des tranches du

14 https://info.adaptivemobile.com/ 5g-network-slicing-security

15 *Denial of Service*

16 https://www.enisa.europa.eu/publications/sdn-threat-landscape

17 https://www.enisa.europa.eu/news/enisa-news/5g

18 https://www.pwc.fi/en/publications/the-practical-pitfalls-of-the-eus-enisa-5g-security-requirements.html

19 *Denial of Slice Service*

20 *Network Slice Manager Impersonation*

réseau V2X fournissant des services différents. Ces véhicules peuvent créer un tunnel pour partager les tranches entre eux. En d'autres termes, les véhicules auront un accès non autorisé aux tranches réseau qui ne leur sont pas attachées.

• **Étanchéité entre les tranches** [21] **:** Comme un véhicule peut être attaché à plusieurs tranches simultanément, les véhicules malveillants peuvent exploiter cette fonctionnalité pour violer l'isolement des tranches réseau.

• **Attaque de brouillage sélectif** [22] **:** contrairement aux attaques traditionnelles de brouillage, cette attaque vise les ressources du *slicing* véhiculaire. Plusieurs véhicules peuvent collaborer ou alterner pour effectuer cette attaque, ce qui la rend difficile à détecter.

• **Écoute clandestine du réseau** [23] **:** L'attaquant recueille des données concernant une tranche de réseau V2X particulière pour en extraire des informations qui peuvent être exploitées. Par exemple, l'attaquant exploite le trafic non chiffré diffusé par les véhicules pour suivre la trajectoire de ses victimes.

Les attaques de brouillage sélectif peuvent directement perturber les communications entre les véhicules et les autres entités. Pour nos deux premiers cas d'usages, une telle perturbation peut avoir des conséquences catastrophiques. L'attaque par usurpation d'identité du gestionnaire de tranches peut permettre à l'attaquant de prendre le contrôle de la gestion des tranches et peut entraîner des conséquences similaires, voire plus graves, que les attaques susmentionnées dans les trois cas d'usage. En comparaison, les attaques d'accès non autorisé aux tranches, d'étanchéité entre les tranches et d'écoute clandestine exposent des informations privées à l'attaquant, qui peut les utiliser pour perturber le fonctionnement normal du système.

Dans le troisième cas d'usage vu plus haut, un groupe de nœuds malveillants pourrait abuser du système de protection du VRU pour surcharger le serveur MEC, retarder la communication et perturber considérablement le trafic. On peut, par exemple, imaginer un scénario dans lequel un ou plusieurs nœuds (malveillants) diffusent de fausses alarmes avec de multiples identités/localisations usurpées pour signaler la présence de nombreux usagers vulnérables dans la zone. Le traitement lié par exemple à la prédiction dynamique du mouvement de ces nombreux usagers consommera une grosse partie des ressources de calcul du serveur MEC. En outre, le trafic malveillant sera amplifié par le serveur MEC et les autres nœuds en raison de la diffusion ultérieure de messages de coordination des manœuvres, de messages de perception collective et de messages d'alerte pour signaler les situations de danger, ce qui dégradera la performance de la tranche de réseau sous-jacente et d'autres tranches qui partagent la même infrastructure physique. Enfin, les fausses alarmes peuvent déclencher des actions simultanées d'évitement des collisions (freinage d'urgence ou ralentissement), ce qui entraîne d'importantes perturbations du trafic.

Des défis transfrontaliers particuliers

Pour les cas d'usage mentionnés précédemment, lorsque la communication se fait avec la technologie 5G, il est prévu que les liens de communication soient sécurisés avec confidentialité et intégrité. Par conséquent, les attaques telles que l'écoute clandestine peuvent être évitées. En effet, les véhicules peuvent s'appuyer sur le protocole TLS [24] (ou DTLS [25]) pour sécuriser leur communication avec l'infrastructure. Cependant, la communication entre les véhicules et d'autres entités telles que les VRUs peut ne pas être en mesure d'utiliser directement TLS ou DTLS, étant donné qu'une infrastructure à clé publique *PKI* [26] commune peut ne pas être disponible, ou qu'une forte exigence de confidentialité/anonymat peut exister dans ce cas. Dans tous les cas, des mécanismes de sécurité doivent être mis en œuvre, faute de quoi les fonctionnalités envisagées ne seront pas correctement réalisées. Nous considérons qu'il s'agit là du premier défi pour les cas d'usage décrits dans cet article.

Lorsque les mécanismes de sécurité 5G et V2X sont activés, il peut y avoir des chevauchements ou des redondances entre les mécanismes de protection à différentes couches. Cela peut poser un problème de violation de la vie privée : si l'on considère à la fois la connexion 5G et l'application, il y aura une authentification du véhicule à la connexion au réseau 5G ; pour l'application V2X, l'utilisateur du véhicule ou le véhicule lui-même procédera généralement à une authentification mutuelle avec le serveur de l'application. Dans ce cas, deux identités seront utilisées et quelqu'un pourrait être en mesure de relier ces identités, et déterminer qu'elles appartiennent au même utilisateur (cyberattaques inter-couches). Avec des mécanismes de confidentialité et d'intégrité appropriés, nous pensons que certaines de ces attaques pourraient être atténuées.

Pour faciliter la discussion, nous faisons la distinction entre les attaquants internes et externes :

- pour un attaquant externe, les attaques les plus réalistes qui peuvent être menées sont le brouillage et les attaques par déni de service. L'impact peut être un retard dans la réception des messages et/ou une perturbation des services pour les victimes ciblées. L'attaquant externe peut également mener une attaque d'écoute pour collecter passivement le trafic réseau et donc être en mesure de déduire certaines informations privées des utilisateurs ;

21 en anglais, *Sealing between slices*

22 en anglais : *Selective jamming attack*

23 en anglais : *Eavesdropping*

24 en anglais : *Transport Layer Security*

25 en anglais : *Datagram TLS*

26 en anglais, *Public Key Infrastructure*

"Les systèmes de détection basés sur le ML/DL doivent être conçus de manière efficace pour couvrir les différentes attaques de slicing véhiculaire. "

- pour un attaquant interne, toutes les attaques peuvent être pertinentes. Cependant, si nous supposons que toutes les communications passent par des canaux sécurisés, l'atténuation de certains comportements malveillants peut être simple. Cependant, les attaquants peuvent injecter de fausses informations sans être directement détectés. Par exemple, les solutions de sécurité traditionnelles ne peuvent pas atténuer les attaques d'envoi de localisation erronée. La détection et l'atténuation de ces attaques internes nécessitent des solutions plus sophistiquées décrites dans un paragraphe suivant. De plus, des compromis entre la sécurité et la confidentialité peuvent être nécessaires dans ce cas, car la révélation d'informations d'identité peut poser des problèmes de confidentialité.

Dans le cadre transfrontalier, deux aspects sont primordiaux. Premièrement, il faut maintenir des canaux de sécurité transparents entre les participants, par exemple entre un véhicule enregistré auprès d'un opérateur mobile et un MEC enregistré auprès d'un autre opérateur mobile. Sans une configuration adéquate et une gestion interopérable des certificats, le risque d'interruption de service est élevé. L'autre aspect est la nécessité de détecter conjointement les attaques (par exemple, le brouillage et le DoSS) par toutes les entités au-delà des frontières. Il y aura également de graves problèmes de confidentialité lorsque des données privées sont nécessaires pour alimenter des solutions basées sur l'apprentissage automatique. En outre, la prévention d'attaques telles que l'étanchéité (*sealing*) entre tranches peut dépendre des politiques de sécurité des opérateurs mobiles concernés. Il est donc important d'avoir une compensation de la faiblesse de la sécurité d'un opérateur par le renforcement des mesures de sécurité à prendre par l'opérateur de l'autre côté de la frontière.

Questions ouvertes, défis et solutions potentielles

Cette section aborde certains des défis liés à la sécurité du *slicing* véhiculaire dans les zones transfrontalières, tout en mettant en évidence les solutions de sécurité potentielles.

Apprentissage automatique pour la détection des attaques

La protection contre des attaques sur le *slicing* véhiculaire, notamment dans les zones transfrontalières, est fastidieuse en raison des techniques avancées utilisées par les attaquants pour s'adapter aux mécanismes de sécurité. Des outils d'apprentissage automatique [27] (ML) ou d'apprentissage profond [28] (DL) ont émergé pour relever ces défis. Cependant, étant donnée la complexité du système, les systèmes de détection basés sur le ML/DL doivent être conçus de manière efficace pour couvrir les différentes attaques de *slicing* véhiculaire. En particulier, l'architecture ML/DL centralisée ne peut pas gérer de tels systèmes complexes en raison de leur rigidité et de leurs limites. En revanche, les algorithmes de ML/DL collaboratifs et distribués sont plus adaptés à la construction de systèmes collaboratifs de détection d'attaques. L'apprentissage fédéré [29] (FL), que nous détaillons ci-après, est un exemple d'apprentissage collaboratif qui permettrait aux opérateurs mobiles d'origine et de destination de collaborer à la construction de modèles de détection d'attaques sans partager leurs données.

Blockchain et « *deception security* » pour l'atténuation des attaques

Si l'on considère que les véhicules ou les VRUs traversent les frontières d'un pays, l'opérateur mobile visité doit leur attribuer une tranche réseau ayant les mêmes caractéristiques que celle affectée par l'opérateur mobile d'origine. Ainsi, l'interconnexion des opérateurs nécessite l'instauration d'un climat de confiance entre eux afin d'assurer la fourniture continue des services et d'empêcher les attaquants d'exploiter ce point d'interconnexion pour casser ou perturber la tranche réseau. À cette fin, la *Blockchain* et les contrats intelligents [30] pourraient être les meilleurs candidats pour établir la confiance entre les opérateurs et protéger les systèmes de détection d'attaques basés sur des algorithmes d'apprentissage ML/DL [12]. Cependant, les solutions basées sur les *blockchains* doivent faire face à des obstacles propres au contexte, tels que les problèmes d'évolutivité liés à l'augmentation du nombre d'utilisateurs et les problèmes de politique, de législation et de réglementation des réseaux de communication mobiles, étant donné que les opérateurs mobiles d'origine et destination appartiennent à des domaines administratifs distincts. Les *blockchains* de consortium pourraient être un catalyseur, permettant à des nœuds sélectionnés (MEC par exemple) par chaque opérateur de créer et de valider des blocs et de les insérer dans la *Blockchain* à l'aide de protocoles de consensus légers tels que le dBFT [31]. Le dBFT offre un débit élevé et un temps de consensus rapide tout en étant hautement tolérant aux pannes. Cependant, l'opérateur mobile d'origine et celui de destination doivent se mettre d'accord sur les données à mettre dans la *Blockchain* afin de respecter les réglementations en matière de confidentialité dans chaque pays. En outre, les contrats intelligents doivent être soigneusement conçus pour respecter

27 en anglais, *Machine Learning*

28 en anglais, *Deep Learning*

29 en anglais, *Federated Learning*

30 en anglais, *smart contracts*

31 *Delegated Byzantine Fault Tolerance*

l'accord sur le niveau de service (SLA [32]) de la tranche de réseau et les politiques réglementaires de chaque pays d'origine et du pays visité.

Une autre approche pour atténuer les attaques est la *Deception* ou *Deceptive Security*, qui vise à ralentir, piéger, dévier et empêcher un intrus d'accéder au système d'information d'une entité. Les pots de miel [33] sont l'un des outils puissants pour mettre en œuvre une stratégie de ce type [13]. Par exemple, nous pouvons déployer un pot de miel distribué composé d'un faux nœud MEC qui imite le comportement du nœud réel, avec de faux *gNodeBs* et de faux véhicules pour détourner les attaquants de la cible réelle et rediriger le trafic malveillant. Il est également possible de mettre en place une fausse tranche réseau ou d'en créer une avec une petite partie des ressources physiques pour isoler et atténuer l'action des attaquants. On pourra ensuite étudier comment ces derniers procèdent pour obtenir un accès non autorisé. Le principal défi à relever ici est de savoir quel est l'emplacement optimal des pots de miel pour en améliorer l'utilité tout en réduisant les faux positifs de la redirection du trafic légitime vers les pots de miel.

Apprentissage fédéré pour la protection de la vie privée

La protection de la vie privée est un autre défi auquel est confronté le *slicing* aux frontières. Comme décrit plus haut, les véhicules et VRUs partagent leurs informations sensibles avec les nœuds MEC pour l'analyse et la prise de décision dans les cas d'usage susmentionnés en utilisant des approches d'apprentissage ML/DL. L'échange d'informations entre les nœuds MEC de l'opérateur mobile d'origine et de l'opérateur destination est essentiel pour assurer aux usagers une continuité de service sans heurts lors du passage aux frontières des deux pays. Ainsi, la détection et l'atténuation des attaques au niveau des MEC sont primordiales, en particulier dans les zones transfrontalières. D'autre part, les nœuds MEC de chaque opérateur mobile (d'origine/destination) stockent des données sensibles (par exemple, les trajectoires passées ou informations sur la mobilité/localisation des utilisateurs) de la route. Le partage de ces données avec les nœuds MEC d'un autre opérateur peut violer la protection de la vie privée des utilisateurs. Le défi consiste donc à garantir les services lors du passage de la frontière sans partager les données entre les opérateurs.

L'apprentissage fédéré (FL) pourrait être une solution prometteuse pour relever ce défi [11]. En effet, les nœuds MEC peuvent former leurs modèles locaux en exploitant les données locales, puis partager uniquement les paramètres des modèles ML/DL pour construire des modèles globaux adaptés aux services véhiculaires. Par conséquent, différents modèles d'apprentissage peuvent être générés aux frontières sans partager de données privées relatives aux deux parties. En outre, le calcul multipartite sécurisé (en anglais, *Secure Multi-MParty Computation*) est une approche cryptographique intéressante dont l'objectif est de permettre aux agents d'un réseau de communication de calculer conjointement une fonction sur leurs entrées, afin que les entrées restent privées et que le résultat soit exact. Il permet ainsi aux MECs de construire ou de tester conjointement des modèles ML en utilisant leurs ensembles de données privées de manière distribuée sans les révéler aux uns et aux autres.

Conclusion

La sécurisation du *slicing* véhiculaire dans la zone transfrontalière est un défi. Alors que les organismes de normalisation progressent dans le domaine de la sécurité des réseaux 5G, la question de la sécurité des réseaux V2X dans les zones transfrontalières n'est pas encore abordée. Cet article t identifie quelques services embarqués pertinents dans ce contexte et décrit des attaques sur le *slicing* véhiculaire en accordant une attention particulière aux zones transfrontalières. Enfin, il aborde les défis liés à la sécurité et à la confidentialité tout en identifiant les questions ouvertes et les opportunités du *slicing* véhiculaire dans des zones transfrontalières, en mettant l'accent sur la détection des attaques, leur atténuation et les solutions potentielles pour la protection de la vie privée. ■

Les auteurs

Abdelwahab Boualouache est chercheur associé à l'Université du Luxembourg.

Sidi Mohammed Senouci est professeur à l'université de Bourgogne.

Bouziane Brik est maitre de conférences à l'université de Bourgogne.

Shajjad Hossain est doctorant à l'Université de Bourgogne.

Qiang Tang est chercheur au LIST.

Abdelaziz Amara Korba est chercheur à l'université de la Rochelle.

Rami Langar est professeur à l'Université Gustave Eiffel depuis 2016, et à l'École de Technologie Supérieure, Montréal (Canada) depuis 2021.

Sylvain Cherrier est maitre de conférences à l'Université Gustave Eiffel.

Badre Bousalem est doctorant à l'Université Gustave Eiffel.

Vinicius F. Silva est chercheur associé à l'Université Gustave Eiffel.

Yacine Ghamri-Doudane est professeur à l'Université de La Rochelle.

Thomas Engel est professeur à l'Université du Luxembourg.

Remerciements

Ce travail a été soutenu par le projet 5G-INSIGHT (ID : 14891397) / (ANR-20-CE25-0015-16) financé par le Fonds National de la Recherche (FNR) au Luxembourg, et par l'Agence Nationale de la Recherche (ANR) en France.

32 *Service-level Agreement*

33 en anglais, *honeypots*

Références

[1] A. Alalewi, I. Dayoub, and S. Cherkaoui, "On 5G-V2X Use Cases and Enabling Technologies: A Comprehensive Survey," IEEE Access, vol. 9, pp. 107 710–107 737, 2021.
[2] D. Garcia-Roger, E. E. Gonza´lez, D. Mart´ın- Sacrista´n, and J.F. Monserrat, "V2x support in 3gpp specifications: From 4g to 5g and beyond," IEEE access, vol. 8, pp. 190 946–190 963, 2020.
[3] I. Afolabi, T. Taleb, K. Samdanis, A. Ksentini, and H. Flinck, "Network Slicing and Softwarization: A Survey on Principles, Enabling Technologies, and Solutions," IEEE Communications Surveys Tutorials, vol. 20, no. 3, pp. 2429–2453, 2018.
[4] "Intelligent transport systems (its); security; threat, vulnerability and risk analysis (tvra)," ETSI TR 102 893 V1.2.1, Tech. Rep., Mar 2017.
[5] "Study on security aspects of enhanced network slicing," 3GPP TR 33.813, V0.8.0, Tech. Rep., Nov 2019.
[6] Kousaridas, M. Fallgren, E. Fischer, F. Moscatelli, R. Vilalta, M. Mu¨hleisen, S. Barmpounakis, X. Vilajosana, S. Euler, B. Tossou, and J. Alonso-Zarate, "5G Vehicle- to-Everything Services in Cross-Border Environments: Standardization and Challenges," IEEE Communications Standards Magazine, vol. 5, no. 1, pp. 22–30, 2021
[7] J. Navarro-Ortiz, P. Romero-Diaz, S. Sendra, P. Ameigeiras, J. J. Ramos-Munoz, and J. M. Lopez-Soler, "A survey on 5g usage scenarios and traffic models," IEEE Communications Surveys & Tutorials, vol. 22, no. 2, pp. 905–929, 2020.
[8] 3GPP TR 22.886, "Study on enhancement of 3GPP Support for 5G V2X Services," Dec 2018.
[9] G. M. Køien, "On Threats to the 5G Service Based Architecture," Wireless Personal Communications, vol. 119, no. 1, pp. 97–116, 2021.
[10] R. F. Olimid and G. Nencioni, "5G Network Slicing: A Security Overview," IEEE Access, vol. 8, pp. 99 999–100 009, 2020.
[11] J. Posner, L. Tseng, M. Aloqaily, and Y. Jararweh, "Federated learning in vehicular networks: opportunities and solutions," IEEE Network, vol. 35, no. 2, pp. 152–159, 2021.
[12] M. A. Togou, T. Bi, K. Dev, K. McDonnell, A. Milenovic, H. Tewari, and G.-M. Muntean, "DBNS: A distributed blockchain-enabled network slicing framework for 5G networks," IEEE Communications Magazine, vol. 58, no. 11, pp. 90– 96, 2020.
[13] S. Panda, S. Rass, S. Moschoyiannis, K. Liang, G. Loukas, and E. Panaousis, "HoneyCar: A Framework to Configure Honeypot Vulnerabilities on the Internet of Vehicles," arXiv preprint arXiv:2111.02364, 2021.

Résumé

Les communications 5G véhiculaires (5G-V2X) continueront à jouer un rôle essentiel dans le développement de l'industrie automobile. En effet, grâce entre autres au concept de découpage du réseau 5G en plusieurs sous-réseaux, de nouveaux cas d'usage futuristes pourront être pris en charge sur un même réseau physique. Cependant, l'utilisation du découpage du réseau 5G-V2X entraîne de nouveaux défis en matière de cybersécurité que les standards actuels, que ce soit ceux du domaine automobile que ceux de la 5G, n'ont pas encore traités. Un élément de vulnérabilité particulier est celui des environnements transfrontaliers où il est nécessaire d'assurer une transition optimale pour les véhicules d'un opérateur à un autre. Cet article vise donc à examiner les problèmes de sécurité et de protection de la vie privée du réseau 5G-V2X tout en recensant les questions ouvertes et les opportunités en zones transfrontalières, en mettant l'accent sur la détection des attaques, leur atténuation et les solutions potentielles pour la protection de la vie privée. ■

Abstract

5G Vehicle-to-Everything (5G-V2X) communications will play a vital role in the development of the automotive industry. Indeed, and thanks to the Network Slicing (NS) concept of 5G networks, unprecedented new vehicular use–cases can be supported on top of the same physical network. However, enabling NS in 5G-V2X brings new security challenges and requirements that automotive or 5G standards have not yet addressed. Furthermore, the attacks can be more powerful, especially if they are produced in cross-border areas of two countries, which require an optimal network transition from one operator to another. Therefore, this article aims to discuss 5G-V2X security and privacy challenges while identifying open issues and opportunities in cross-border areas, with a focus on attack detection, their mitigation, and privacy protection potential solutions. ■